HL7 Privacy and Security Vocabulary Tables

August 29, 2012

Table of Contents

[HL7 Privacy and Security Vocabulary Enumeration Diagram 2](#_Toc334016968)

[Confidentiality 2](#_Toc334016970)

[v:Confidentiality 2.16.840.1.113883.5.25 2](#_Toc334016971)

[v:x\_BasicConfidentialityKind:2.16.840.1.113883.1.11.16926 3](#_Toc334016972)

[v:x\_VeryBasicConfidentialityKind:2.16.840.1.113883.1.11.19738 4](#_Toc334016973)

[Purpose of Use 4](#_Toc334016974)

[ActConsentType 6](#_Toc334016975)

[ActPolicyType Definitions 7](#_Toc334016976)

[InformationSensitivityPolicy 8](#_Toc334016977)

[ActInformationSensitivityPolicy 10](#_Toc334016978)

[EntityInformationSensitivityPolicyType 11](#_Toc334016979)

[RoleInformationSensitivityPolicy 12](#_Toc334016980)

[ActSecurityPolicy – ObligationPolicy 13](#_Toc334016981)

[ActSecurityPolicy – RefrainPolicy 14](#_Toc334016982)

# HL7 Privacy and Security Vocabulary Enumeration Diagram

# 

# Confidentiality

### v:Confidentiality 2.16.840.1.113883.5.25

*Definition:* Privacy metadata indicating the sender's sensitivity classification, which is based on an analysis of applicable privacy policies and the risk of harm that could result from unauthorized disclosure.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lvl- Typ** | **Concept Code *Head Code-defined Value Set*** | **Print Name** | **Definition, Properties, Relationships** |
| 0-**S** | **\_Confidentiality** | Confidentiality | **Definition:** Privacy metadata indicating the sender's sensitivity classification, which is based on an analysis of applicable privacy policies and the risk of harm that could result from unauthorized disclosure.  *Map:* Definition aligns with ISO 7498-2:1989 - Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.  *Usage Note:* Confidentiality codes are used as metadata indicating the receiver responsibilities to ensure that the information is not made available or redisclosed to unauthorized individuals, entities, or processes (security principals) per applicable policies.  **Concept Relationships:** **Generalizes (derived):** L M N R U V |
| 1-**L** | . **L** | low | **Definition:** Privacy metadata indicating that the information has been de-identified, and there are mitigating circumstances that prevent re-identification, which minimize risk of harm from unauthorized disclosure. The information requires protection to maintain low sensitivity.  *Examples:* Includes anonymized, pseudonymized, or non-personally identifiable information such as HIPAA limited data sets.  *Map:* No clear map to ISO 13606-4 Sensitivity Level (1) Care Management: RECORD\_COMPONENTs that might need to be accessed by a wide range of administrative staff to manage the subject of care's access to health services.  *Usage Note:* This metadata indicates the receiver may have an obligation to comply with a data use agreement. |
| 1-**L** | . **M** | moderate | **Definition:** Privacy metadata indicating moderately sensitive information, which presents moderate risk of harm if disclosed without authorization.  *Examples:* Includes allergies of non-sensitive nature used inform food service; health information a patient authorizes to be used for marketing, released to a bank for a health credit card or savings account; or information in personal health record systems that are not governed under health privacy laws.  *Map:* Partial Map to ISO 13606-4 Sensitivity Level (2) Clinical Management: Less sensitive RECORD\_COMPONENTs that might need to be accessed by a wider range of personnel not all of whom are actively caring for the patient (e.g. radiology staff).  *Usage Note:* This metadata indicates that the receiver may be obligated to comply with the receiver's terms of use or privacy policies. |
| 1-**L** | . **N** | normal | **Definition:** Privacy metadata indicating that the information is typical, non-stigmatizing health information, which presents typical risk of harm if disclosed without authorization.  *Examples:* In the US, this includes what HIPAA identifies as the minimum necessary protected health information (PHI) given a covered purpose of use (treatment, payment, or operations). Includes typical, non-stigmatizing health information disclosed in an application for health, workers compensation, disability, or life insurance.  *Map:* Partial Map to ISO 13606-4 Sensitivity Level (3) Clinical Care: Default for normal clinical care access (i.e. most clinical staff directly caring for the patient should be able to access nearly all of the EHR). Maps to normal confidentiality for treatment information but not to ancillary care, payment and operations.  *Usage Note:* This metadata indicates that the receiver may be obligated to comply with applicable jurisdictional privacy law or disclosure authorization. |
| 1-**L** | . **R** | restricted | **Definition:** Privacy metadata indicating highly sensitive, potentially stigmatizing information, which presents a high risk to the information subject if disclosed without authorization. May be preempted by jurisdictional law, e.g., for public health reporting or emergency treatment.  **Examples:**  Includes information related to mental health, HIV, substance abuse, domestic violence, child abuse, genetic disease, and reproductive health. May be used to indicate proprietary or classified information that is not related to an individual, e.g., secret ingredients in a therapeutic substance; or the name of a manufacturer.  **Partial Map to** ISO 13606-4 Sensitivity Level (4) Privileged Care:   Access restricted to a small group of people caring intimately for the patient, perhaps an immediate care team or senior clinical party (the privileged clinical setting needs to be specified e.g. mental health).  **Usage Note:**   This metadata indicates that the receiver may be obligated to comply with the information subject’s consent directive or jurisdictional or organizational policies that are more stringent than prevailing or default jurisdictional privacy laws. |
| 1-**L** | . **U** | unrestricted | **Definition:** Privacy metadata indicating that the information is not classified as sensitive.  *Examples:* Includes publicly available information, e.g., business name, phone, email or physical address.  *Usage Note:* This metadata indicates that the receiver has no obligation to consider additional policies when making access control decisions. Note that in some jurisdictions, personally identifiable information must be protected as confidential, so it would not be appropriate to assign a confidentiality code of "unrestricted" to that information even if it is publicly available. |
| 1-**L** | . **V** | very restricted | **Definition:** Privacy metadata indicating extremely sensitive, likely stigmatizing information, which presents a very high risk if disclosed without authorization.  This information must be kept in the highest confidence.  **Examples:** Includes information about a victim of abuse, patient requested information sensitivity, and taboo subjects relating to health status that must be discussed with the patient by an attending provider before sharing with the patient.  May also include information held under “legal lock” or attorney-client privilege.  **Usage Note:**   This metadata indicates that the receiver may not disclose this information except as directed by the information custodian, who may be the information subject.  **Partial Map** toISO 13606-4 Sensitivity Level (5) Personal Care:    To be shared by the subject of care perhaps with only one or two other people whom they trust most, or only accessible to the subject of care (and to others by one-off authorizations). |

## V:x\_BasicConfidentialityKind:2.16.840.1.113883.1.11.16926

|  |  |
| --- | --- |
| . N | normal |
| . **R** | restricted |
| . **V** | very restricted |

## V:x\_VeryBasicConfidentialityKind:2.16.840.1.113883.1.11.19738

|  |  |
| --- | --- |
| . N | normal |
| . **R** | restricted |

# Purpose of Use

C:ActReason:PurposeOfUse:23408

V:PurposeOfUse:2.16.840.1.113883.1.11.20448

V:GeneralPurposeOfUse:2.16.840.1.113883.1.11.20449

|  |  |  |  |
| --- | --- | --- | --- |
| **Lvl- Typ** | **Concept Code *Head Code-defined Value Set*** | **Print Name** | **Definition, Properties, Relationships** |
| For XSPA – use General Purpose of Use value set, which is the subset of the POU codes below in tan colored rows. | | | |
| 2-**A** | . . **PurposeOfUse**  [*v:*](file:///C:\..\..\Desktop\HL7\HL7%20Normative%20Edition%202011%20CD1\Edition2011\infrastructure\vocabulary\vs_ActReason.html#ActConsentInformationAccessOverrideReason)*PurposeOfUse; v:GeneralPurposeOfUse* | purpose of use | **Definition:** Reason for performing one or more operations on information, which may be permitted by source system’s security policy in accordance with one or more privacy policies and consent directives. Description: The rationale or purpose for an act relating to the management of personal health information, such as collecting personal health information for research or public health purposes.  **Concept Relationships:** **Specializes:** \_ActHealthInformationManagementReason **Generalizes (derived):** TREAT HPAYMT HOPERAT HMARKT HRESCH PATRQT |
| 3-**S** | . . . **HMARKT** | healthcare marketing | **Definition:** To perform one or more operations on information for marketing services and products related to health care. |
| 3-**S** | . . . **HOPERAT** | healthcare operations | **Definition:** To perform one or more operations on information used for conducting administrative and contractual activities related to the provision of health care.  **Concept Relationships:** **Specializes:** PurposeOfUse **Generalizes (derived):** DONAT FRAUD GOV HACCRED HCOMPL HDECD HDIRECT HLEGAL HOUTCOMS HPRGRP HQUALIMP HSYSADMIN MEMADMIN PATADMIN PATSFTY PERFMSR RECORDMGT TRAIN |
| 4-**L** | . . . . **DONAT** | donation | **Definition:** To perform one or more operations on information used for cadaveric organ, eye or tissue donation. |
| 4-**L** | . . . . **FRAUD** | fraud | **Definition:** To perform one or more operations on information used for fraud detection and prevention processes. |
| 4-**L** | . . . . **GOV** | government | **Definition:** To perform one or more operations on information used within government processes. |
| 4-**L** | . . . . **HACCRED** | accreditation | **Definition:** To perform one or more operations on information for conducting activities related to meeting accreditation criteria. |
| 4-**L** | . . . . **HCOMPL** | compliance | **Definition:** To perform one or more operations on information used for conducting activities required to meet a mandate. |
| 4-**L** | **….HDECD** | decedent | **Definition:** To perform one or more operations on information used for handling deceased patient matters. |
| 4-**L** | **….HDIRECT** | directory | **Definition:** To perform one or more operation operations on information used to manage a patient directory. Examples: Facility, enterprise, payer, or health information exchange patient directory. |
| 4-**L** | . . . . **HLEGAL** | legal | **Definition:** To perform one or more operations on information for conducting activities required by legal proceeding. |
| 4-**L** | . . . . **HOUTCOMS** | outcome measure | **Definition:** To perform one or more operations on information used for assessing results and comparative effectiveness achieved by health care practices and interventions. |
| 4-**L** | . . . . **HPRGRP** | program reporting | **Definition:** To perform one or more operations on information used for conducting activities to meet program accounting requirements. |
| 4-**L** | . . . . **HQUALIMP** | quality improvement | **Definition:** To perform one or more operations on information used for conducting administrative activities to improve health care quality. |
| 4-**L** | . . . . **HSYSADMIN** | system administration | **Definition:** To perform one or more operations on information to administer the electronic systems used for the delivery of health care. |
| 4-**L** | . . . . **MEMADMIN** | member administration | **Definition:**  To perform one or more operations on information to administer health care coverage to an enrollee under a policy or program. |
| 4-**L** | . . . . **PATADMIN** | patient administration | **Definition:** To perform one or more operations on information used for operational activities conducted to administer the delivery of health care to a patient. |
| 4-**L** | . . . . **PATSFTY** | patient safety | **Definition:** To perform one or more operations on information in processes related to ensuring the safety of health care. |
| 4-**L** | . . . . **PERFMSR** | performance measure | **Definition:** To perform one or more operations on information used for monitoring performance of recommended health care practices and interventions. |
| 4-**L** | . . . . **RECORDMGT** | records management | **Definition:** To perform one or more operations on information used within the health records management process. |
| 4-**L** | . . . . **TRAIN** | training | **Definition:** To perform one or more operations on information used in training and education. |
| 3-**S** | . . . **HPAYMT** | healthcare payment | **Definition:** To perform one or more operations on information for conducting financial or contractual activities related to payment for provision of health care.  **Concept Relationships:** **Specializes:** PurposeOfUse **Generalizes (derived):** ELIGDTRM CLMATTCH COVAUTH REMITADV |
| 4-**L** | . . . . **COVERAGE** | coverage under policy or program | **Definition:** To perform one or more operations on information for conducting activities related to coverage under a program or policy. |
| 5-**L** | . . . . . **ELIGDTRM** | eligibility determination | **Definition:** To perform one or more operations on information used for conducting eligibility determination for coverage in a program or policy. May entail review of financial status or disability assessment. |
| 5-**L** | . . . . . **ELIGVER** | eligibility verification | **Definition:** To perform one or more operations on information used for conducting eligibility verification of coverage in a program or policy. May entail provider contacting coverage source (e.g., government health program such as workers compensation or health plan) for confirmation of enrollment, eligibility for specific services, and any applicable copays. |
| 5-**L** | . . . . . **ENROLLM** | enrollment | **Definition:** To perform one or more operations on information used for enrolling a covered party in a program or policy. May entail recording of covered party’s and any dependent’s demographic information and benefit choices. |
| 4-**L** | . . . . **CLMATTCH** | claim attachment | **Definition:** To perform one or more operations on information for provision of additional clinical evidence in support of a request for coverage or payment for health services. |
| 4-**L** | . . . . **COVAUTH** | coverage authorization | **Definition:** To perform one or more operations on information for conducting prior authorization or predetermination of coverage for services. |
| 4-**L** | . . . . **REMITADV** | remittance advice | **Definition:** To perform one or more operations on information about the amount remitted for a health care claim. |
| 3-**S** | . . . **HRESCH** | healthcare research | **Definition:** To perform one or more operations on information for conducting scientific investigations to obtain health care knowledge.  **Concept Relationships:** **Specializes:** PurposeOfUse  **Generalizes (derived):** CLINTRCH |
| 4-**L** | . . . . **CLINTRCH** | clinical trial research | **Definition:** To perform one or more operations on information for conducting scientific investigations in accordance with clinical trial protocols to obtain health care knowledge. |
| 3-**S** | . . . **PATRQT** | patient requested | **Definition:** To perform one or more operations on information in response to a patient's request.  **Concept Relationships:** **Specializes:** PurposeOfUse  **Generalizes (derived):** FAMRQT PWATRNY SUPNWK |
| 4-**L** | **. . . . FAMRQT** | family requested | **Definition:** To perform one or more operations on information in response to a request by a family member authorized by the patient. |
| 4-**L** | . . . . **PWATRNY** | power of attorney | **Definition:** To perform one or more operations on information in response to a request by a person appointed as the patient's legal representative. |
| 4-**L** | . . . . **SUPNWK** | support network | **Definition:** To perform one or more operations on information in response to a request by a person authorized by the patient. |
| 3-**S** | . . . **PUBHLTH** |  | **Definition:** To perform one or more operations on information for conducting public health activities, such as the reporting of notifiable conditions.  **Concept Relationships:** **Specializes:** PurposeOfUse  **Generalizes (derived):** DISASTER THREAT |
| 4-**L** | . . . . **DISASTER** |  | **Definition:** To perform one or more operations on information used for provision of immediately needed health care to a population of living subjects located in a disaster zone. |
| 4-**L** | . . . . **THREAT** |  | **Definition:** To perform one or more operations on information used to prevent injury or disease to living subjects who may be the target of violence. |
| 3-**S** | . . . **TREAT** | treatment | **Definition:** To perform one or more operations on information for provision of health care.  **Concept Relationships:** **Specializes:** PurposeOfUse  **Generalizes (derived):** CAREMGT CLINTRL ETREAT POPHLTH |
| 4-**L** | . . . . **CAREMGT** | care management treatment | **Definition:** To perform one or more operations on information for provision of health care coordination. |
| 4-**L** | . . . . **CLINTRL** | clinical trial treatment | **Definition:** To perform one or more operations on information for provision of health care within a clinical trial. |
| 4-**L** | . . . . **ETREAT** | emergency treatment | **Definition:** To perform one or more operations on information for provision of immediately needed health care for an emergent condition. |
| 4-**L** | . . . . **POPHLTH** | population health treatment | **Definition:** To perform one or more operations on information for provision of health care to a population of living subjects, e.g., needle exchange program. |

# ActConsentType

V:ActConsentType:2.16.840.1.113883.1.11.19897

Note that this differs from the list of ActConsentDirective codes highlighted below

|  |  |  |  |
| --- | --- | --- | --- |
| **Lvl** | **ActCode System** | **Print Name** | **Definition** |
| 0-**A** | **\_ActConsentType** [*v:ActConsentType*](http://www.hl7.org/v3ballotarchive_temp_D909B368-1C23-BA17-0CE13B52122CE1B6/v3ballot2012may/html/infrastructure/vocabulary/vs_ActCode.html#ActConsentType) | ActConsentType | **Definition:** The type of consent directive, e.g., to consent or dissent to collect, access, or use in specific ways within an EHRS or for health information exchange; or to disclose health information for purposes such as research.  **Concept Relationships:** **Generalizes (derived):** ICOL IDSCL INFA IRDSCL RESEARCH **ClassifiesClassCode to:** CONS |
| 1-**L** | . **ICOL** | information collection | **Definition:** Consent to have healthcare information collected in an electronic health record. This entails that the information may be used in analysis, modified, updated. |
| 1-**L** | . **IDSCL** | information disclosure | **Definition:** Consent to have collected healthcare information disclosed. |
| 1-**S** | . **INFA** *.* [*v:ActInformationAccess*](http://www.hl7.org/v3ballotarchive_temp_D909B368-1C23-BA17-0CE13B52122CE1B6/v3ballot2012may/html/infrastructure/vocabulary/vs_ActCode.html#ActInformationAccess) | information access | **Definition:** Consent to access healthcare information.  **Concept Relationships:** **Specializes:** \_ActConsentType **Generalizes (derived):** INFAO INFASO |
| 2-**L** | . . **INFAO** | access only | **Definition:** Consent to access or "read" only, which entails that the information is not to be copied, screen printed, saved, emailed, stored, re-disclosed or altered in any way. This level ensures that data which is masked or to which access is restricted will not be. **Example:** Opened and then emailed or screen printed for use outside of the consent directive purpose. |
| 2-**L** | . . **INFASO** | access and save only | **Definition:** Consent to access and save only, which entails that access to the saved copy will remain locked. |
| 1-**L** | . **IRDSCL** | information redisclosure | **Definition:** Information re-disclosed without the patient's consent. |
| 1-**S** | . **RESEARCH** *.* [*v:ActResearchInformationAccess*](http://www.hl7.org/v3ballotarchive_temp_D909B368-1C23-BA17-0CE13B52122CE1B6/v3ballot2012may/html/infrastructure/vocabulary/vs_ActCode.html#ActResearchInformationAccess) | research information access | **Definition:** Consent to have healthcare information in an electronic health record accessed for research purposes.  **Concept Relationships:** **Specializes:** \_ActConsentType **Generalizes (derived):** RSDID RSREID |
| 2-**L** | . . **RSDID** | de-identified information access | **Definition:** Consent to have de-identified healthcare information in an electronic health record that is accessed for research purposes, but without consent to re-identify the information under any circumstance. |
| 2-**L** | . . **RSREID** | re-identifiable information access | **Definition:** Consent to have de-identified healthcare information in an electronic health record that is accessed for research purposes re-identified under specific circumstances outlined in the consent.  **Example:** Where there is a need to inform the subject of potential health issues. |

# ActPolicyType Definitions

C:ActCode:\_ActPolicyType:22182

V:ActPolicyType:2.16.840.1.113883.1.11.19886

|  |  |  |  |
| --- | --- | --- | --- |
| **Lvl** | **ActCode System** | **Print Name** | **Definition** |
| **0-A** | \_Act Policy Type | Act Policy Type | Types of policies that further specify the ActClassPolicy value set. |
| **1-L** | \_ActPrivacyPolicyType | ActPrivacyPolicyType | Definition: A mandate, obligation, requirement, rule, or expectation relating to privacy.  Description: A policy deeming certain information to be private to an individual or organization.  Discussion: ActPrivacyPolicyType codes support the designation of the 1…\* policies that are applicable to an Act such as a Consent Directive, a Role such as a VIP Patient, or an Entity such as a patient who is a minor. 1…\* ActPrivacyPolicyType values may be associated with an Act or Role to indicate the policies that govern the assignment of an Act or Role confidentialityCode. Use of multiple ActPrivacyPolicyType values enables fine grain specification of applicable policies, but must be carefully assigned to ensure cogency and avoid creation of conflicting policy mandates. Usage Note: Statutory title may be named in the ActClassPolicy Act Act.title to specify which privacy policy is being referenced. |
| **2-A** | \_ActConsentDirective | ActConsentDirective | Definition: Specifies the type of consent directive indicated by an ActClassPolicy e.g., a 3rd party authorization to disclose or consent for a substitute decision maker (SDM) or a notice of privacy policy. Usage Note: ActConsentDirective codes are used to specify the type of Consent Directive to which a Consent Directive Act conforms. |
| **3-L** | EMRGONLY | emergency only | Definition: Opt-in to disclosure of health information for emergency only consent directive. Description: This general consent directive specifically limits disclosure of health information for purpose of emergency treatment. Additional parameters may further limit the disclosure to specific users, roles, duration, types of information, and impose uses obligations. |
| **3-L** | . NOPP | notice of privacy practices | Definition: Acknowledgement of custodian notice of privacy practices. Description: This type of consent directive acknowledges a custodian’s notice of privacy practices including its permitted collection, access, use and disclosure of health information to users and for purposes of use specified. |
| **3-L** | OPTIN | opt-in | Definition: Opt-in to disclosure of health information consent directive. Description: This general consent directive permits disclosure of health information. Additional parameter may limit authorized users, purpose of use, user obligations, duration, or information types permitted to be disclosed, and impose uses obligations. |
| **3-L** | OPTOUT | opt-out | Definition: Opt-out of disclosure of health information consent directive. Description: This general consent directive prohibits disclosure of health information. Additional parameters may permit access to some information types by certain users, roles, purposes of use, durations and impose user obligations. |
| **2-A** |  | Act Privacy Law | Definition: A jurisdictional mandate relating to privacy.  Usage Note: May be used to bind realm specific privacy law code systems such as the ActUSPrivacyLaw code system to create a realm specific value set. |
| **0-A** | .Act US Privacy Law  (Note – US Realm Only) | Act US Privacy Law | Definition: A jurisdictional mandate in the U.S. relating to privacy. Usage Note: ActPrivacyLaw codes may be associated with an Act or a Role to indicate the legal provision to which the assignment of an Act.confidentialityCode or Role.confidentialtyCode complies. May be used to further specify rationale for assignment of other ActPrivacyPolicy codes in the US realm, e.g., ETH and 42CFRPart2 can be differentiated from ETH and Title38Part1. |
|  |  | 42 CFR Part2 | Definition: Non-disclosure of health information relating to health care paid for by a federally assisted substance abuse program without patient consent. Description: 42 CFR Part 2 stipulates the right of an individual who has applied for or been given diagnosis or treatment for alcohol or drug abuse at a federally assisted program  Usage Notes: May be associated with an Act or a Role to indicate the legal provision to which the assignment of an Act.confidentialityCode or Role.confidentialtyCode complies. |
| **1-L** |  | Common Rule | Definition: U.S. federal laws governing research-related privacy policies. Description: U.S. Federal regulations governing the protection of human subjects in research (codified at Subpart A of 45 CFR part 46) that has been adopted by 15 U.S. Federal departments and agencies in an effort to promote uniformity, understanding, and compliance with human subject protections. Existing regulations governing the protection of human subjects in Food and Drug Administration (FDA)-regulated research (21 CFR parts 50, 56, 312, and 812) are separate from the Common Rule but include similar requirements. Usage Notes: May be associated with an Act or a Role to indicate the legal provision to which the assignment of an Act.confidentialityCode or Role.confidentialtyCode complies. |
| **1-L** |  | HIPAA notice of privacy practices | Definition: Notification of HIPAA Privacy Practices. Description: The U.S. Public Law 104-191 Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 CFR Part 164 Subpart E) permits access, use and disclosure of certain personal health information (PHI as defined under the law) for purposes of Treatment, Payment, and Operations, and requires that the provider ask that patients acknowledge the Provider’s Notice of Privacy Practices as permitted conduct under the law. Usage Notes: May be associated with an Act or a Role to indicate the legal provision to which the assignment of an Act.confidentialityCode or Role.confidentialtyCode complies. |
| **1-L** |  | HIPAA psychotherapy notes | Definition: Authorization that must be obtained for disclosure of psychotherapy notes. Description: The U.S. Public Law 104-191 Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 CFR Part 164 Section 164.508) requires authorization for certain uses and disclosure of psychotherapy notes. Usage Notes: May be associated with an Act or a Role to indicate the legal provision to which the assignment of an Act.confidentialityCode or Role.confidentialtyCode complies. |
| **1-L** |  | HIPAA self-pay | Definition: Non-disclosure of health information to a health plan relating to health care items or services for which an individual pays out of pocket in full. Description: Section 13405(a) of the Health Information Technology for Economic and Clinical Health Act (HITECH) stipulates the right of an individual to have disclosures regarding certain health care items or services for which the individual pays out of pocket in full restricted from a health plan. Usage Notes: May be associated with an Act or a Role to indicate the legal provision to which the assignment of an Act.confidentialityCode or Role.confidentialtyCode complies. |
| **1-L** | .Title 38 Section 7332 | Title 38 Section 7332 | Definition: Title 38 Part 1 protected information may only be disclosed to a third party with the special written consent of the patient except where expressly authorized by 38 USC 7332. VA may disclose this information for specific purposes to: VA employees on a need to know basis - more restrictive than Privacy Act need to know; contractors who need the information in order to perform or fulfill the duties of the contract; and researchers who provide assurances that the information will not be identified in any report. This information may also be disclosed without consent where patient lacks decision-making capacity; in a medical emergency for the purpose of treating a condition which poses an immediate threat to the health of any individual and which requires immediate medical intervention; for eye, tissue, or organ donation purposes; and disclosure of HIV information for public health purposes.  Description: Title 38 Part 1 - §1.462 Confidentiality restrictions.  *(a)General.* The patient records to which §§1.460 through 1.499 of this part apply may be disclosed or used only as permitted by these regulations and may not otherwise be disclosed or used in any civil, criminal, administrative, or legislative proceedings conducted by any Federal, State, or local authority. Any disclosure made under these regulations must be limited to that information which is necessary to carry out the purpose of the disclosure. SUBCHAPTER III--PROTECTION OF PATIENT RIGHTS Sec. 7332. Confidentiality of certain medical records (a)(1) Records of the identity, diagnosis, prognosis, or treatment of any patient or subject which are maintained in connection with the performance of any program or activity (including education, training, treatment, rehabilitation, or research) relating to drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus, or sickle cell anemia which is carried out by or for the Department under this title shall, except as provided in subsections (e) and (f), be confidential, and (section 5701 of this title to the contrary notwithstanding) such records may be disclosed only for the purposes and under the circumstances expressly authorized under subsection (b). Usage Notes: May be associated with an Act or a Role to indicate the legal provision to which the assignment of an Act.confidentialityCode or Role.confidentialtyCode complies. |

# InformationSensitivityPolicy

V:InformationSensitivityPolicy 2.16.840.1.113883.1.11.20428

|  |  |  |  |
| --- | --- | --- | --- |
| **Lvl** | **ActCode System** | **Print Name** | **Definition** |
| 2-**S** | \_InformationSensitivityPolicy | InformationSensitivityPolicy | A mandate, obligation, requirement, rule, or expectation characterizing the value or importance of a resource and may include its vulnerability (Based on ISO7498-2:1989). Note: The vulnerability of personally identifiable sensitive information may be based on concerns that the unauthorized disclosure may result in social stigmatization or discrimination.) Description: Types of Sensitivity policy that apply to Acts or Roles. A sensitivity policy is adopted by an enterprise or group of enterprises (a policy domain) through a formal data use agreement that stipulates the value, importance, and vulnerability of information. A sensitivity code representing a sensitivity policy may be associated with criteria such as categories of information or sets of information identifiers (e.g., a value set of clinical codes or branch in a code system hierarchy). These criteria may in turn be used for the Policy Decision Point in a Security Engine. A sensitivity code may be used to set the confidentiality code used on information about Acts and Roles to trigger the security mechanisms required to control how security principals (i.e., a person, a machine, a software application) may act on the information (e.g., collection, access, use, or disclosure). Sensitivity codes are never assigned to the transport or business envelope containing patient specific information being exchanged outside of a policy domain as this would disclose the information intended to be protected by the policy. When sensitive information is exchanged with others outside of a policy domain, the confidentiality code on the transport or business envelope conveys the receiver’s responsibilities and indicates the how the information is to be safeguarded without unauthorized disclosure of the sensitive information. This ensures that sensitive information is treated by receivers as the sender intends, accomplishing interoperability without point to point negotiations.  **Description:** A sensitivity policy is adopted by an enterprise or group of enterprises (a "policy domain") through a formal data use agreement that stipulates the value, importance, and vulnerability of information. A sensitivity code representing a sensitivity policy may be associated with criteria such as categories of information or sets of information identifiers (e.g., a value set of clinical codes or branch in a code system hierarchy). These criteria may in turn be used for the Policy Decision Point in a Security Engine. A sensitivity code may be used to set the confidentiality code used on information about Acts and Roles to trigger the security mechanisms required to control how security principals (i.e., a person, a machine, a software application) may act on the information (e.g., collection, access, use, or disclosure). Sensitivity codes are never assigned to the transport or business envelope containing patient specific information being exchanged outside of a policy domain as this would disclose the information intended to be protected by the policy. When sensitive information is exchanged with others outside of a policy domain, the confidentiality code on the transport or business envelope conveys the receiver's responsibilities and indicates the how the information is to be safeguarded without unauthorized disclosure of the sensitive information. This ensures that sensitive information is treated by receivers as the sender intends, accomplishing interoperability without point to point negotiations  **Usage Notes:** Sensitivity codes are not useful for interoperability outside of a policy domain without an out-of-band agreement on semantics because sensitivity policies are typically localized and vary drastically across policy domains even for the same information category because of differing organizational business rules, security policies, and jurisdictional requirements. For example, an employee sensitivity code (EMPL) would make little sense for use outside of a policy domain. The code “taboo” (TBOO) would rarely be useful outside of a policy domain unless there are jurisdictional requirements requiring that a provider disclose sensitive information to a patient directly. Sensitivity codes may be more appropriate in a legacy system’s Master Files in order to notify those who access a patient’s orders and observations about the sensitivity policies that apply. Newer systems may have a security engine that uses sensitivity policy criteria directly. The specializable InformationSensitivityPolicy Act.code may be useful in some scenarios if used in combination with a sensitivity identifier and/or Act.title. |
| 3-**L** | .ADOL | adolescent information sensitivity | Policy for handling information related to an adolescent, which will be afforded heightened confidentiality per applicable organizational or jurisdictional policy. Description: An enterprise may have a policy that requires that adolescent patient information be provided heightened confidentiality. Information deemed sensitive typically includes health information and patient role information including patient status, demographics, next of kin, and location.  **Usage Notes:** For use within an enterprise in which an adolescent is the information subject. If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 3-**L** | .CEL | celebrity information sensitivity | Policy for handling information related to a celebrity (people of public interest (VIP), which will be afforded heightened confidentiality. Description: Celebrities are people of public interest (VIP) about whose information an enterprise may have a policy that requires heightened confidentiality. Information deemed sensitive may include health information and patient role information including patient status, demographics, next of kin, and location.  **Usage Notes:** For use within an enterprise in which the information subject is deemed a celebrity or very important person. If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 3-**L** | .DIA | diagnosis information sensitivity | Policy for handling information related to a diagnosis, health condition or health problem, which will be afforded heightened confidentiality. Description: Diagnostic, health condition or health problem related information may be deemed sensitive by organizational policy, and require heightened confidentiality.  **Usage Notes**: For use within an enterprise that provides heightened confidentiality to diagnostic, health condition or health problem related information deemed sensitive. If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 3-**L** | .DRGIS | drug information sensitivity | Policy for handling information related to a drug, which will be afforded heightened confidentiality. Description: Drug information may be deemed sensitive by organizational policy, and require heightened confidentiality.  **Usage Notes:** For use within an enterprise that provides heightened confidentiality to drug information deemed sensitive. If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 3-**L** | .EMP | employee information sensitivity | Policy for handling information related to an employee, which will be afforded heightened confidentiality. Description: When a patient is an employee, an enterprise may have a policy that requires heightened confidentiality. Information deemed sensitive typically includes health information and patient role information including patient status, demographics, next of kin, and location.  **Usage Notes:** For use within an enterprise that employs the information subject. If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 3-**L** | .PRD | patient default sensitivity | Policy for handling information reported by the patient about another person, e.g., a family member, which will be afforded heightened confidentiality. Description: Sensitive information reported by the patient about another person, e.g., family members may be deemed sensitive by default. The flag may be set or cleared on patient's request.  **Usage Notes:** For sensitive information relayed by or about a patient, which is deemed sensitive within the enterprise (i.e., by default regardless of whether the patient requested that the information be deemed sensitive.) If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 3-**L** | .PRS | patient requested sensitivity | Information deemed sensitive by the patient for which the patient requests and will be afforded heightened confidentiality. Description: Patient may deem patient role and health information sensitive for which the patient may request and receive heightened confidentiality. Information deemed sensitive may include health information and patient role information including patient status, demographics, next of kin, and location. For example, a patient may request that sensitive information is not to be shared with family members. Typically, information reported by the patient about family members is sensitive by default. Flag can be set or cleared on patient's request.  **Usage Notes:** For use within an enterprise that provides heightened confidentiality to certain types of information designated by a patient as sensitive. If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |

# ActInformationSensitivityPolicy

V:ActInformationSensitivityPolicy 2.16.840.1.113883.1.11.20428

|  |  |  |  |
| --- | --- | --- | --- |
| **Lvl** | **ActCode System** | **Print Name** | **Definition** |
| 3-**A** | \_ActInformationSensitivityPolicy | ActInformationSensitivityPolicy | Types of sensitivity policies that apply to Acts. Description: Act.confidentialityCode is defined in the RIM as “constraints around appropriate disclosure of information about this Act, regardless of mood.”  **Usage Notes:** ActSensitivity codes are used to bind information to an Act.confidentialityCode according to local sensitivity policy so that those confidentiality codes can then govern its handling across enterprises. Internally to a policy domain, however, local policies guide the access control system on how end users in that policy domain are able to use information tagged with these sensitivity values. |
| 4-**L** | .ETH | substance abuse information sensitivity | Policy for handling alcohol or drug-abuse information, which will be afforded heightened confidentiality. Description: Information handling protocols based on organizational policies related to alcohol or drug-abuse information that is deemed sensitive.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .GDIS | genetic disease information sensitivity | Policy for handling genetic disease information, which will be afforded heightened confidentiality. Description: Information handling protocols based on organizational policies related to genetic disease information that is deemed sensitive.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .HIV | HIV/AIDS information sensitivity | Policy for handling HIV or AIDS information, which will be afforded heightened confidentiality. Description: Information handling protocols based on organizational policies related to HIV or AIDS information that is deemed sensitive.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .PSY | psychiatry information sensitivity | Policy for handling psychiatry information, which will be afforded heightened confidentiality. Description: Information handling protocols based on organizational policies related to psychiatry information that is deemed sensitive.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .SDV | sexual assault, abuse, or domestic violence information sensitivity | Policy for handling sexual assault, abuse, or domestic violence information, which will be afforded heightened confidentiality. Description: Information handling protocols based on organizational policies related to sexual assault, abuse, or domestic violence information that is deemed sensitive.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-L | .SEX | sexuality and reproductive health information sensitivity | Policy for handling sexuality and reproductive health information, which will be afforded heightened confidentiality. Description: Information handling protocols based on organizational policies related to sexuality and reproductive health information that is deemed sensitive.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .STD | sexually transmitted disease information sensitivity | Definition: Policy for handling sexually transmitted disease information, which will be afforded heightened confidentiality.  Description: Information handling protocols based on organizational policies related to sexually transmitted disease information that is deemed sensitive.  Usage Notes: If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .TBOO | taboo | Definition: Policy for handling information not to be initially disclosed or discussed with patient except by a physician assigned to patient in this case.  Description: Information handling protocols based on organizational policies related to sensitive patient information that must be initially discussed with the patient by an attending physician before being disclosed to the patient.  Usage Notes: This is usually a temporary policy constraint only, and the sensitivity classification will likely change once the provider has discussed the information with the patient or other information subject. If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |

# EntityInformationSensitivityPolicyType

V: EntityInformationSensitivityPolicy 2.16.840.1.113883.1.11.20431

|  |  |  |  |
| --- | --- | --- | --- |
| **Lvl** | **ActCode System** | **Print Name** | **Definition** |
| 3-**A** | \_EntityInformationSensitivityPolicyType | EntityInformationSensitivityPolicy | Types of sensitivity policies that may apply to a sensitive attribute on an Entity.  **Usage Notes:** EntitySensitivity codes are used to convey a policy that is applicable to sensitive information conveyed by an entity attribute. May be used to bind a Role.confidentialityCode associated with an Entity per organizational policy. Role.confidentialityCode is defined in the RIM as “an indication of the appropriate disclosure of information about this Role with respect to the playing Entity.” |
| 4-**L** | .DEMO | all demographic information sensitivity | Policy for handling all demographic information about an information subject, which will be afforded heightened confidentiality. Description: Policies may govern sensitivity of information related to all demographic about an information subject, the disclosure of which could impact the privacy, well-being, or safety of that subject.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .DOB | date of birth information sensitivity | Policy for handling information related to an information subject’s date of birth, which will be afforded heightened confidentiality. Description: Policies may govern sensitivity of information related to an information subject’s date of birth, the disclosure of which could impact the privacy, well-being, or safety of that subject.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .GENDER | gender and sexual orientation information sensitivity | Policy for handling information related to an information subject’s gender and sexual orientation, which will be afforded heightened confidentiality. Description: Policies may govern sensitivity of information related to an information subject’s gender and sexual orientation, the disclosure of which could impact the privacy, well-being, or safety of that subject.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .LIVARG | living arrangement information sensitivity | Policy for handling information related to an information subject’s living arrangement, which will be afforded heightened confidentiality. Description: Policies may govern sensitivity of information related to an information subject’s living arrangement, the disclosure of which could impact the privacy, well-being, or safety of that subject.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .MARST | marital status information sensitivity | Policy for handling information related to an information subject’s marital status, which will be afforded heightened confidentiality. Description: Policies may govern sensitivity of information related to an information subject’s marital status, the disclosure of which could impact the privacy, well-being, or safety of that subject.  **Usage Notes**: If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition this more generic code. |
| 4-**L** | .RACE | race information sensitivity | Policy for handling information related to an information subject’s race, which will be afforded heightened confidentiality. Description: Policies may govern sensitivity of information related to an information subject’s race, the disclosure of which could impact the privacy, well-being, or safety of that subject.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .REL | religion information sensitivity | Policy for handling information related to an information subject’s religious affiliation, which will be afforded heightened confidentiality. Description: Policies may govern sensitivity of information related to an information subject’s religion, the disclosure of which could impact the privacy, well-being, or safety of that subject.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code |

# RoleInformationSensitivityPolicy

V: RoleInformationSensitivityPolicy 2.16.840.1.113883.1.11.20430

|  |  |  |  |
| --- | --- | --- | --- |
| **Lvl** | **ActCode System** | **Print Name** | **Definition** |
| 3-**A** | \_RoleInformationSensitivityPolicy | RoleInformationSensitivityPolicy | Types of sensitivity policies that apply to Roles.  **Usage Notes**: RoleSensitivity codes are used to bind information to a Role.confidentialityCode per organizational policy. Role.confidentialityCode is defined in the RIM as “an indication of the appropriate disclosure of information about this Role with respect to the playing Entity.” |
| 4-**L** | .B | business information sensitivity | Policy for handling trade secrets such as financial information or intellectual property, which will be afforded heightened confidentiality. Description: Since the service class can represent knowledge structures that may be considered a trade or business secret, there is sometimes (though rarely) the need to flag those items as of business level confidentiality.  **Usage Notes:** No patient related information may ever be of this confidentiality level. If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .EMPL | employer information sensitivity | Policy for handling information related to an employer which is deemed classified to protect an employee who is the information subject, and which will be afforded heightened confidentiality. Description: Policies may govern sensitivity of information related to an employer, such as law enforcement or national security, the identity of which could impact the privacy, well-being, or safety of an information subject who is an employee.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code |
| 4-**L** | .LOCIS | location information sensitivity | Policy for handling information related to the location of the information subject, which will be afforded heightened confidentiality. Description: Policies may govern sensitivity of information related to the location of the information subject, the disclosure of which could impact the privacy, well-being, or safety of that subject.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |
| 4-**L** | .SSP | sensitive service provider information sensitivity | Policy for handling information related to a provider of sensitive services, which will be afforded heightened confidentiality. Description: Policies may govern sensitivity of information related to providers who deliver sensitive healthcare services in order to protect the privacy, well-being, and safety of the provider and of patients receiving sensitive services.  **Usage Notes:** If there is a jurisdictional mandate, then use the applicable ActPrivacyLaw code system, and specify the law rather than or in addition to this more generic code. |

# ActSecurityPolicy – ObligationPolicy

V: ObligationPolicy 2.16.840.1.113883.1.11.20445

|  |  |  |  |
| --- | --- | --- | --- |
| **Lvl- Typ** | **Concept Code *Head Code-defined Value Set*** | **Print Name** | **Definition, Properties, Relationships** |
| 0**-A** | **\_ActPolicyType** | Act Policy Type | **Definition:** Types of policies that further specify the ActClassPolicy value set.  **Concept Relationships:** **Generalizes (derived):** COVPOL, ActPrivacyPolicyType, ActConsentDirective, ActSecurityPolicyType **ClassifiesClassCode to:** POLICY |
| 1**-A** | **\_SecurityPolicy**  *v:SecurityPolicy* | security policy | **Definition:** Types of security policies that further specify the ActClassPolicy value set. Example: obligation to encrypt; refrain from redisclosure without consent.  **Concept Relationships: Generalizes (derived):** ObligationPolicy; RefrainPolicy  **Specializes:** ActPolicyType |
| 2**-A** | **\_ObligationPolicy**  *v:ObligationPolicy* | obligation policy | **Definition:** Conveys the mandated workflow action that an information custodian, receiver, or user must perform.  **Description:** Per ISO 22600-2, ObligationPolicy instances 'are event-triggered and define actions to be performed by manager agent'. Per HL7 Composite Security and Privacy Domain Analysis Model: This value set refers to the action required to receive the permission specified in the privacy rule. [Nov Harm - Per OASIS XACML, an obligation is an operation specified in a policy or policy that is performed in conjunction with the enforcement of an access control decision.]  **Concept Relationships: Specializes:** ActSecurityPolicyType  **Generalizes (derived):** AOD ANONY AUDT AUDTR CPLYPOL CPLYCC CPLYCD CPLYJPP CPLYOPP CPLYOSP DEID DELAU ENCRYPT ENCRYPTR ENCRYPTT ENCRYPTU HUAPRV MASK REDACT PSEUD |
| 3**-L** | **…AOD** | accounting of disclosure | **Definition:** Custodian system must make available to an information subject upon request an accounting of certain disclosures of the individual’s protected health information over a period of time. Policy may dictate that the accounting include information about the information disclosed, the date of disclosure, the identification of the receiver, the purpose of the disclosure, the time in which the disclosing entity must provide a response and the time period for which accountings of disclosure can be requested. |
| 3**-L** | **…ANONY** | anonymize | **Definition:** Custodian system must remove any information that could result in identifying the information subject. |
| 3**-L** | **…AUDIT** | audit | **Definition:** Custodian system must monitor systems to ensure that all users are authorized to operate on information objects. |
| 3**-L** | **…AUDTR** | audit trail | **Definition:** Custodian system must monitor and maintain retrievable log for each user and operation on information. |
| 3**-L** | **…CPLYPOL** | comply with policy | **Definition:** Custodian security system must retrieve, evaluate, and comply with applicable policies associated with the target information. |
| 3**-L** | **…CPLYCC** | comply with confidentiality code | **Definition:** Custodian security system must retrieve, evaluate, and comply with the information handling directions of the Confidentiality Code associated with an information target. |
| 3**-L** | **…CPLYCD** | comply with consent directive | **Definition:** Custodian security system must retrieve, evaluate, and comply with applicable information subject consent directives. |
| 3**-L** | **…CPLYJPP** | comply with jurisdictional privacy policy | **Definition:** Custodian security system must retrieve, evaluate, and comply with applicable jurisdictional privacy policies associated with the target information. |
| 3**-L** | **…CPLYOPP** | comply with organizational privacy policy | **Definition:** Custodian security system must retrieve, evaluate, and comply with applicable organizational privacy policies associated with the target information. |
| 3**-L** | **…CPLYOSP** | comply with organizational security policy | **Definition:** Custodian security system must retrieve, evaluate, and comply with the organizational security policies associated with the target information. |
| 3**-L** | **…DEID** | deidentify | **Definition:** Custodian system must strip information of data that would allow the identification of the source of the information or the information subject. |
| 3**-L** | **…DELAU** | delete after use | **Definition:** Custodian system must remove target information from access after use. |
| 3**-L** | **…ENCRYPT** | encrypt | **Definition:** Custodian system must render information unreadable by algorithmically transforming plaintext into ciphertext. Description: A mathematical transposition of a file or data stream so that it cannot be deciphered at the receiving end without the proper key. Encryption is a security feature that assures that only the parties who are supposed to be participating in a videoconference or data transfer are able to do so. It can include a password, public and private keys, or a complex combination of all. (Per Infoway.)  **Concept Relationships: Generalizes (derived):** ObligationPolicy  **Specializes:** ENCRYPTR, ENCRYPTT, ENCRYPTU |
| 3**-L** | **…ENCRYPTR** | encrypt at rest | **Definition:** Custodian system must render information unreadable and unusable by algorithmically transforming plaintext into ciphertext when "at rest" or in storage. |
| 3**-L** | **… ENCRYPTT** | encrypt in transit | **Definition:** Custodian system must render information unreadable and unusable by algorithmically transforming plaintext into ciphertext while "in transit" or being transported by any means. |
| 3**-L** | **…ENCRYPTU** | encrypt in use | **Definition:** Custodian system must render information unreadable and unusable by algorithmically transforming plaintext into ciphertext while in use such that operations permitted on the target information are limited by the license granted to the end user. |
| 3**-L** | **…MASK** | mask | **Definition:** Custodian system must render information unreadable and unusable by algorithmically transforming plaintext into ciphertext. User may be provided a key to decrypt per license or “shared secret”. |
| 3-**L** | **…MINEC** | minimum necessary | Custodian system must limit disclosure to the minimum information required to support an authorized user's purpose of use. |
| 3**-L** | **…REDACT** | redact | **Definition:** Custodian system must remove information, which is not authorized to be access, used, or disclosed from records made available to otherwise authorized users. |
| 3**-L** | **…HUAPRV** | human approval | **Definition:** Custodian system must require human review and approval for permission requested. |
| 3**-L** | **…PSEUD** | pseudonymize | **Definition:** Custodian system must strip information of data that would allow the identification of the source of the information or the information subject. Custodian may retain a key to relink data necessary to reidentify the information subject. |

# ActSecurityPolicy – RefrainPolicy

V: RefrainPolicy 2.16.840.1.113883.1.11.20446

|  |  |  |  |
| --- | --- | --- | --- |
| **Lvl- Typ** | **Concept Code *Head Code-defined Value Set*** | **Print Name** | **Definition, Properties, Relationships** |
| 2**-A** | **\_RefrainPolicy**  *v:RefrainPolicy* | refrain policy | **Definition:** Conveys prohibited actions which an information custodian, receiver, or user is not permitted to perform unless otherwise authorized or permitted under specified circumstances.  **Description:** ISO 22600-2 species that a Refrain Policy “*defines actions the subjects must refrain from performing”.* Per HL7 Composite Security and Privacy Domain Analysis Model: May be used to indicate that a specific action is prohibited based on specific access control attributes e.g., purpose of use, information type, user role, etc.  **Concept Relationships:** **Specializes:** ActSecurityPolicyType  **Generalizes (derived):**  NOAUTH NOCOLLECT NOINTEGRATE NOLIST NOMOU NOORGPOL NOPERSIST NORDSCLW NORELINK NODSCLCD NORDSCLCD NOREUSE |
|  | **NOAUTH** | prohibit disclosure without subject authorization | **Definition:** Prohibition on disclosure without information subject's authorization. |
|  | **NOCOLLECT** | prohibit collection | **Definition:** Prohibition on collection or storage of the information. |
|  | **NODSCLCD** | prohibit disclosure without consent directive | **Definition:** Prohibition on disclosure without organizational approved patient restriction. |
|  | **NOINTEGRATE** | prohibit integration | **Definition:** Prohibition on Integration into other records. |
|  | **NOLIST** | prohibit unlisted entity disclosure | **Definition:** Prohibition on disclosure except to entities on specific access list. |
|  | **NOMOU** | prohibit disclosure without MOU | **Definition:** Prohibition on disclosure without an interagency service agreement or memorandum of understanding (MOU). |
|  | **NOORGPOL** | prohibit disclosure without organizational authorization | **Definition:** Prohibition on disclosure without organizational authorization. |
|  | **NOPERSIST** | prohibit collection beyond purpose of use | **Definition:** Prohibition on collection of the information beyond time necessary to accomplish authorized purpose of use is prohibited. |
|  | **NORDSCLCD** | prohibit redisclosure without consent directive | **Definition:** Prohibition on redisclosure without patient consent directive. |
|  | **NORDSCLW** | prohibit disclosure without jurisdictional authorization | **Definition:** Prohibition on disclosure without authorization under jurisdictional law. |
|  | **NORELINK** | prohibit relinking | **Definition:** Prohibition on associating de-identified or pseudonymized information with other information in a manner that could or does result in disclosing information intended to be masked. |
|  | **NOREUSE** | prohibit reuse beyond purpose of use | **Definition:** Prohibition on use of the information beyond the purpose of use initially authorized. |
|  | **NOVIP** | prohibit unauthorized VIP disclosure | **Definition:** Prohibition on disclosure except to principals with access permission to specific VIP information. |
|  | **ORCON** | prohibit disclosure without originator authorization | **Definition:** Prohibition on disclosure except as permitted by the information originator. |